A Performance Evaluation Study of an X.509 Compliant Public Key Infrastructure

Emilia Rosti

Joint work with Danilo Bruschi and Arianna Curti

Dipartimento di Scienze dell'Informazione

Università degli Studi di Milano

rose@dsi.unimi.it

Outline

- PKI: what it is
- X.509: what it means
- Certificate revocation protocols
- Modeling a PKI
- Results
- Future work

Public Key Infrastructure

- A system comprising policies, software and hardware components that realize a trusted third party that guarantees
  - authenticity,
  - ownership,
  - validity,

  of “keys” and information related to them.
  - implements “organized” trust relationships

PKI - Certificates

- End users generate public-private key pairs
- Certificate associated with public component of each key pair
  - information about owner, certifier entity, certificate validity, algorithm used for signature, digital signature of the certifier entity

PKI - Certificates

- Certificate authenticity
  - issued by PKI
- Certificate ownership
  - binding between certificate and organization (person) indicated on it
- Certificate validity
  - not revoked

PKI - Components

- Registration Authority
  - authenticates users, distributes keys and certificates, requests certificates
- Certification Authority
  - digitally signs, distributes, and revokes certificates, issues lists of revoked certificates
    - trusted third party
- Directory
  - stores certificates for public access
  - X.500 directory with LDAP access protocol

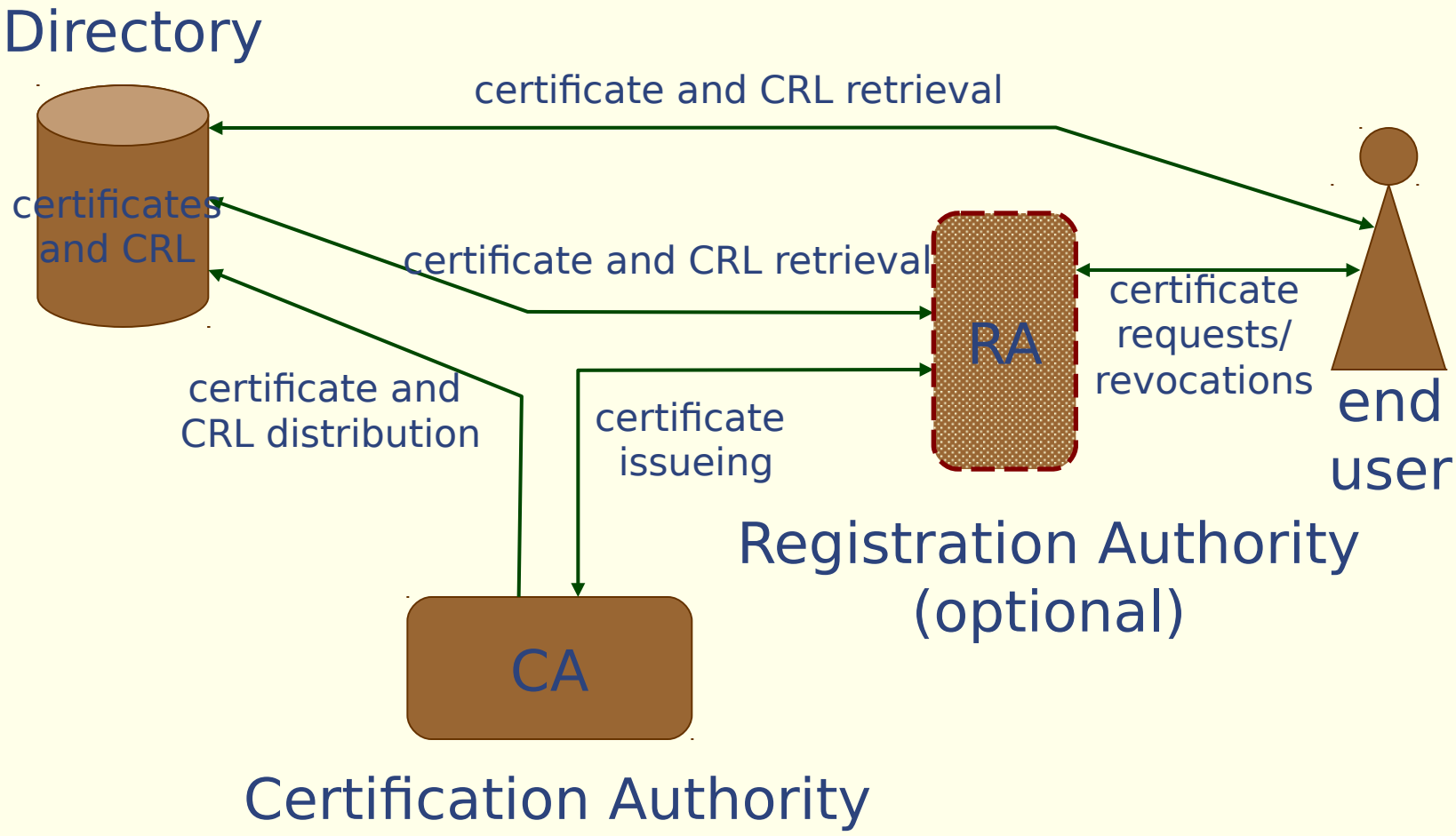
PKI – End users

- People and/or software applications
  - request ceritificate from CA or via RA, access Directory to download lists of revoked certificates and certificates of other party
  - may have SW or HW devices for signature/encryption (smart card)

PKI - Functionalities

- Issueing certificates
- Distributing certificates
- Distributing certificate status information
  - certificate revocation lists (CRLs)
- Distributing policies adopted when issueing certificates

Public Key Infrastructure



X.509

- Standard protocol for authentication services in X.500 Directory Service
  - part of X.500 Directory Recommendation
  - adopted by Visa, Mastercard, Netscape, Entrust, TimeStep

X.509v3

- Current standard
  - extension of X.509
  - more flexible structure
    - from hierarchical structure with three levels

      Internet Policy Registration Authority (root)

      Policy Certification Authorities (level 2)

      Certification Authorities (level 3

      to flat structure with cross certification among CAs
      - no need to traverse the tree up to IPRA

X.509v3 certificate

- (X.509) Information about
  - version and serial number
  - subject (key owner)
  - issuer (CA that issued certificate)
  - validity (not before, not after)
  - subject public key info (key and algorithm to be used with)
  - algorithm used for signing
  - signature of certificate

X.509v3 certificate

- v3 extensions
  - authority key ID (if CA has multiple signature keys)
  - subject key info (if subject has multiple keys)
  - key usage restrictions
  - certificate policies
  - CA and subject attributes
  - certification constraints
  - CRL distribution points

Certificate revocation

- Certificates may be revoked before their natural expiration date
  - private key compromised/lost
  - canceled account
- Certificate status information must be published for end user to be able to verify certificates they handle

Certificate revocation

- Certificate Revocation List
  - serial numbers of revoked certificates
  - time of revocation
  - CA signature
  - CRL issuance time
  - next CRL issuance time
- Size
  - 51B + 9B*#revoked_certificates [MITRE 94]
  - entries deleted after certificate expiration

Certificate revocation protocols

- Periodic publication of CRL
  - possibly outdated information
    - overissued CRL
    - periodic publication of updates (delta-CRL)
- On demand status verification via OCSP (On-line Certificate Status Protocol)
  - timely status information
- Revocation policies performance analysis [Cooper1999, 2000]

Modeling a PKI

- Who
  - CA, RA, Directory, end users
  - does what
    - transaction identification
    - service demands
  - and how
    - different policies for revocation information management

Modeling a PKI

- CA transactions
  - certificate issuance
    - self-signed, RA-generated, renewal
  - cross-certification
  - certificate revocation
  - CRL publication

Modeling a PKI

- RA transactions
  - certificate issuance request
  - certificate revocation request
- Directory transactions
  - search, modify, add, delete
- End users transactions
  - certificate issuance/revocation request
  - certificate status verification

Modeling a PKI - Transactions

- Self-signed certificate requests
  - user generates request and protects it with shared secret
  - CA authenticates sender and shared secret, generates certificate, inserts it in local DB, signs reply and sends it to user
  - user verifies CA signature, sends ack to CA
  - CA publishes certificate in Directory

Modeling a PKI - Transactions

- RA-generated certificate requests
  - RA verifies user request, signs it and sends it to CA
  - CA verifies RA signature, generates certificate, inserts it in local DB, signs and sends it to RA
  - RA verifies CA signature, sends certificate to user, ack to CA
  - CA publishes the certificate in Directory

Modeling a PKI - Transactions

- Self-signed revocation requests
  - user generates revocation request, signs it and sends it to CA
  - CA verifies user's signature, adds serial number and revocation time to local DB, sends signed reply to user
  - user verifies CA signature

Modeling a PKI - Transactions

- RA-generated revocation requests
  - RA generates revocation request, signs it and sends it to CA
  - CA verifies RA signature, adds serial number and revocation time to local DB, sends signed reply to RA
  - RA verifies CA signature and informs user

Modeling a PKI - Transactions

- CRL generation
  - CA reads revocation list, last full CRL and delta-CRL from local DB
  - CA generates new delta-CRL and signs it
  - CA updates local DB
  - CA publishes delta-CRL in Directory

Modeling a PKI - Methodology

- Queueing network model
  - hierarchical analysis
    - components in isolation
    - complete model
    - enhancements
  - analytic and simulation
    - exponentially distributed service times and customers interarrival times
  - single and multiclass customer population
    - different resource usage by various transactions
  - closed and open models

Modeling a PKI - Objectives

- Bottleneck analysis
- Impact of population mix on response time
- Maximum arrival rate for an acceptable response time
- What if analysis

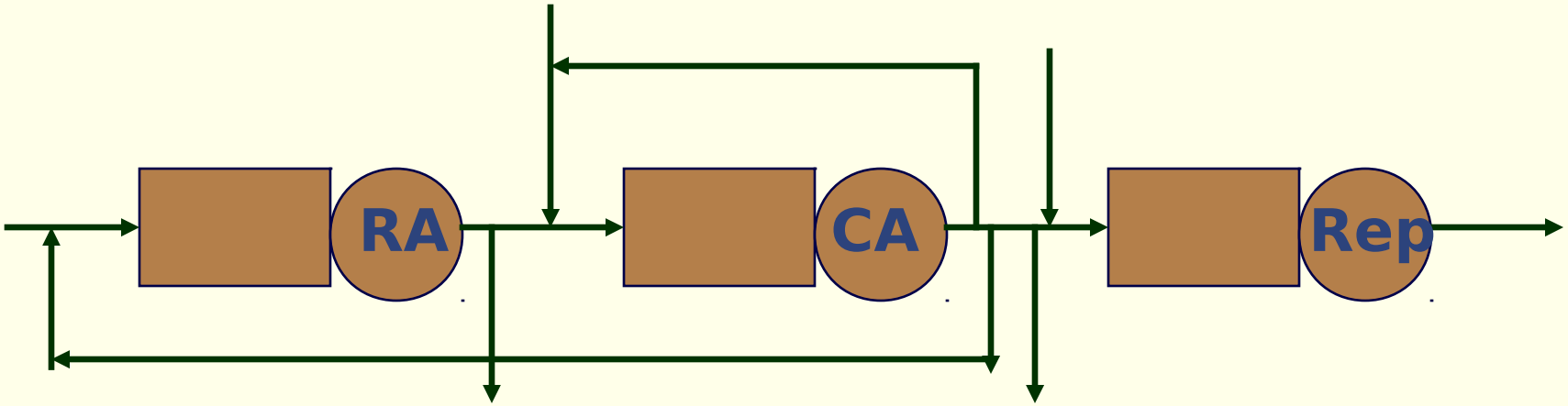
Modeling a PKI - Assumptions

- 2048 RSA bit signature key for CA
  - dedicated cryptographic coprocessor
- MD5 hash
- Simple queries by CA to local certificate DB
- Certificates for signature keys only
- Delta-CRL
- Off-line full CRL generation
- Signed messages
- Network communication services ignored

Modeling a PKI - Assumptions

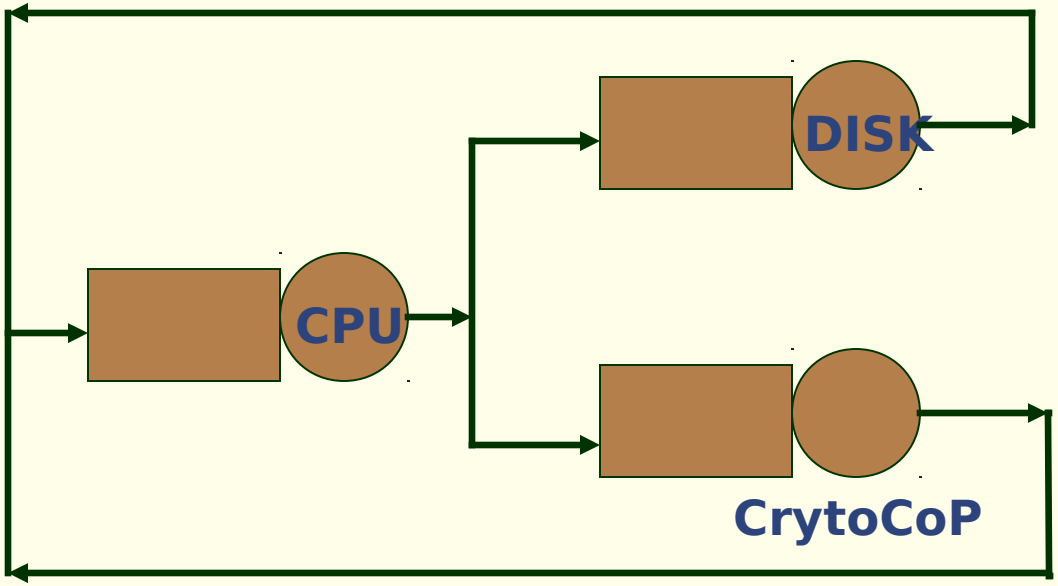
- Multiclass customer population
  - class 1: self-signed certificate request
  - class 2: self-signed revocation request
  - class 3: delta-CRL generation
  - class 4: RA-generated certificate request
  - class 5: RA-generated revocation request
  - class 6: cross-certification request

PKI complete model



Basic models

- CA model in isolation
- RA model in isolation



Basic models parameters

- Number of users/certificates: 50,000
- Avg. number of revoked certificates: 20%
- Service demands estimation (ms)
  - time to sign 166 ms, to verify signature 4 ms

	cl1	cl2	cl3	cl4	cl5	cl6
CAmod						
CPU	0.215	0.049	3.584	0.182	0.051	0.199
DISK	43.163	32.373	44.36	43.167	32.337	32.373
CCP	340	170	166	336	170	336
RAmod						
CPU				0.215	0.081	
DISK				32.835	21.144	
CCP				340	340	

cl1: self-sig. req
cl2: self-sig. rev
cl3: delta-CRL
cl4: RA-gen req.
cl5: RA-gen rev.
cl6: cross-cert.

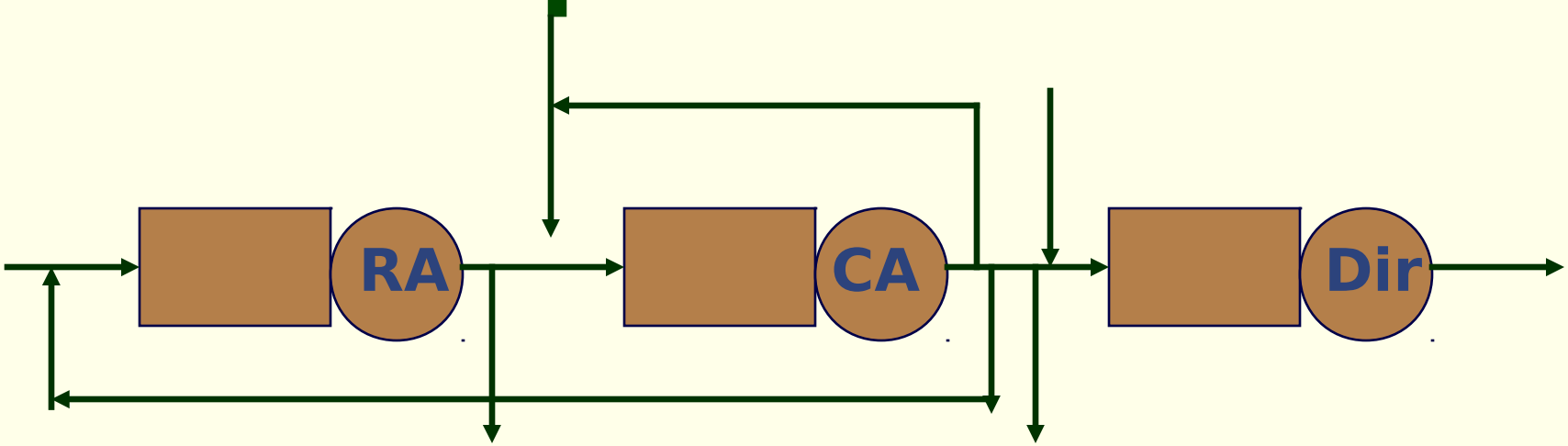
Basic model results

- Signature is the bottleneck operation
- CA and RA can be modeled as load independent servers
  - service rates are throughputs obtained
  - service times in complete model (ms)

	cl1	cl2	cl3	cl4	cl5	cl6
CA	340	170	166	336	170	336
RA				340	340	

cl1: self-sig. req
cl2: self-sig. rev
cl3: delta-CRL
cl4: RA-gen req.
cl5: RA-gen rev.
cl6: cross-cert.

Complete model



- Only 5 classes
  - class 6 accounts for less than 0.02%
- Directory
  - certificate publication: 6ms
  - CRL publication: 12ms

Complete model assumptions

- Variable population mixes on classes 1, 2, 3, 4, 5
  - class 3 arrival rate is fixed
    - generation of delta-CRL every 10 minutes

    $\forall \lambda_3 = 0.001667$ req/s
  - variable splits of total arrival rate λ among classes

    $\forall \lambda_1 = \beta_1(\lambda - \lambda_3)$

    $\forall \lambda_2 = \beta_2(\lambda - \lambda_3)$

    $\forall \lambda_4 = \beta_4(\lambda - \lambda_3)$

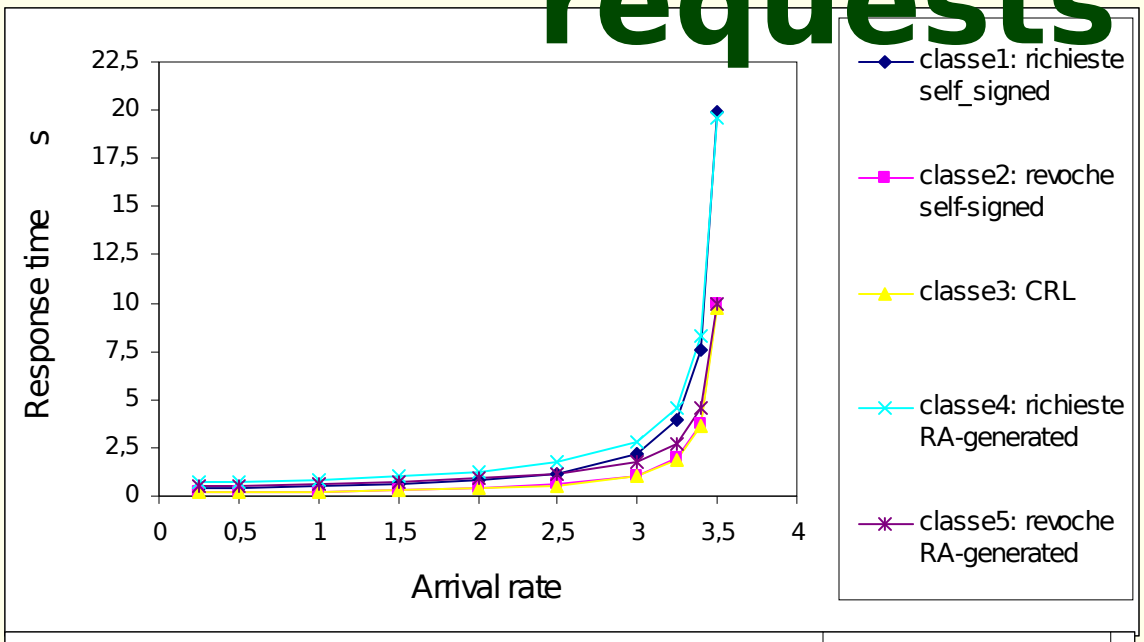
    $\forall \lambda_5 = \beta_5(\lambda - \lambda_3)$

    $\forall \beta_1 + \beta_2 + \beta_4 + \beta_5 = 1$

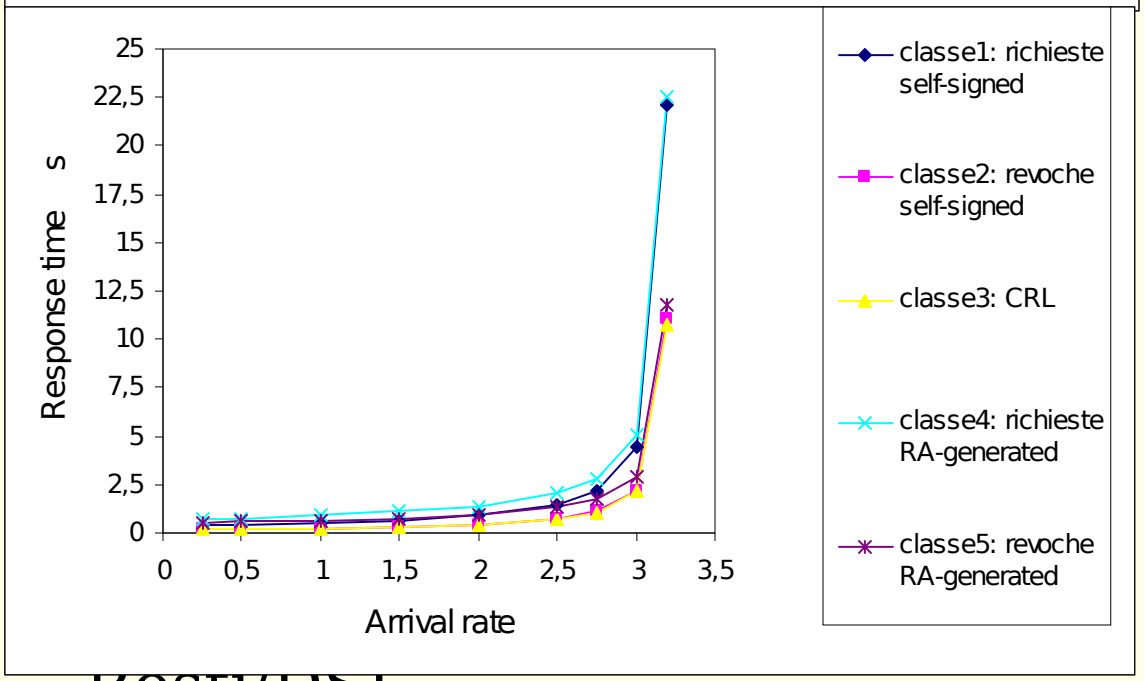
Model results

- Certificate requests rate larger than revocation requests rate
  - very unbalanced: total request fraction 82%
    - $\forall \beta_1 = \beta_4 = 41\%$
    - $\forall \beta_2 = \beta_5 = 9\%$
  - less unbalanced: total request fraction 66%
    - $\forall \beta_1 = \beta_4 = 33\%$
    - $\forall \beta_2 = \beta_5 = 17\%$

More certificate requests



66% new certificate requests
$3 < \lambda_{max} < 3.5$

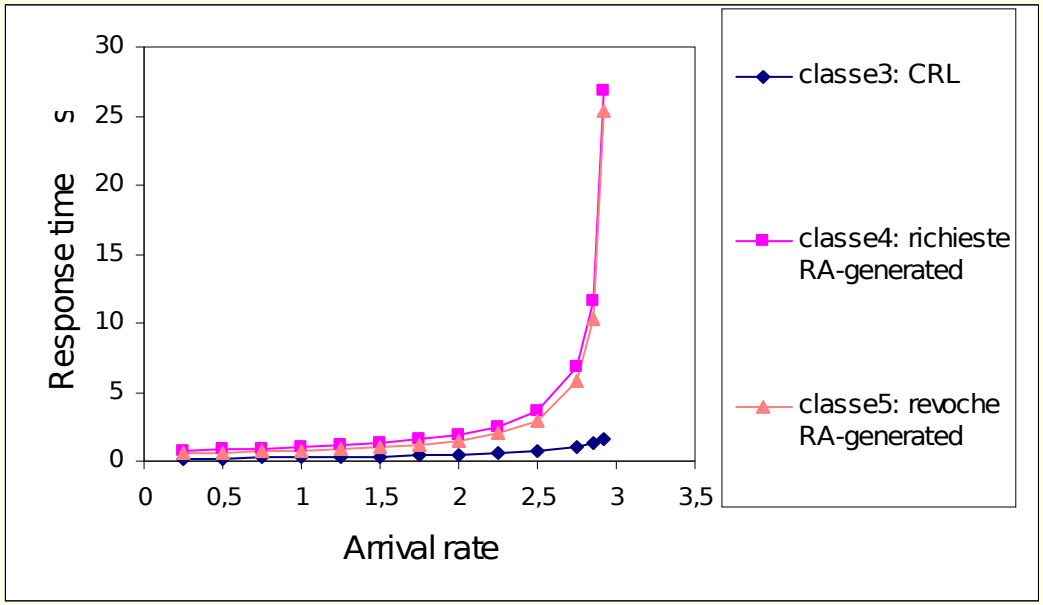


82% new certificate requests
$3 < \lambda_{max} < 3.5$

Model results

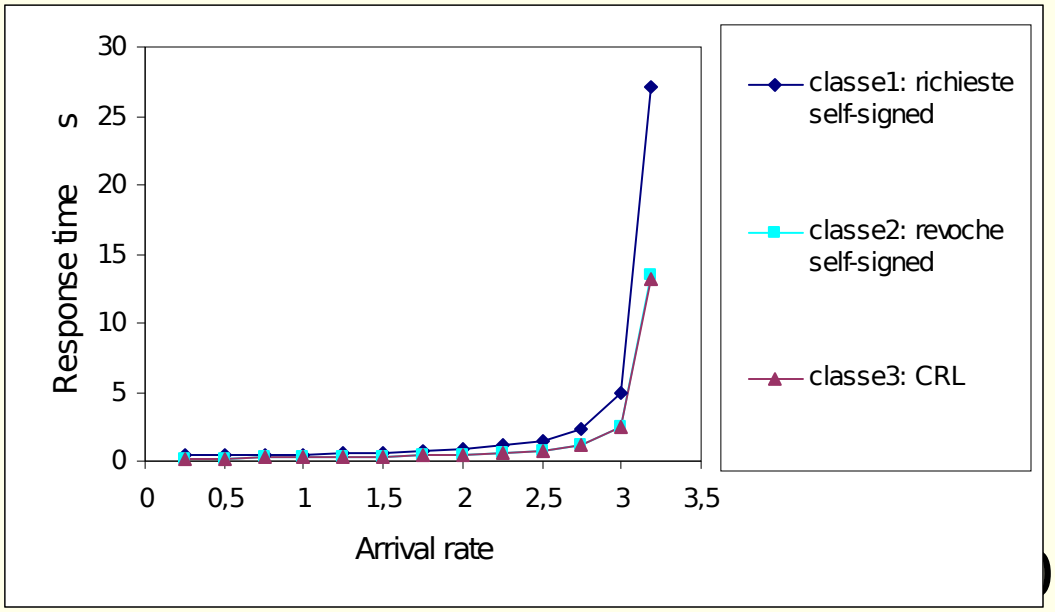
- Only RA-generated certificate and revocation requests
  - $\beta_4 = 82\%$
  - $\beta_5 = 18\%$
- Only self-signed certificate and revocation requests
  - $\beta_1 = 82\%$
  - $\beta_2 = 18\%$

Unique request source



RA-generated only requests

$2.5 < \lambda_{max} < 3$



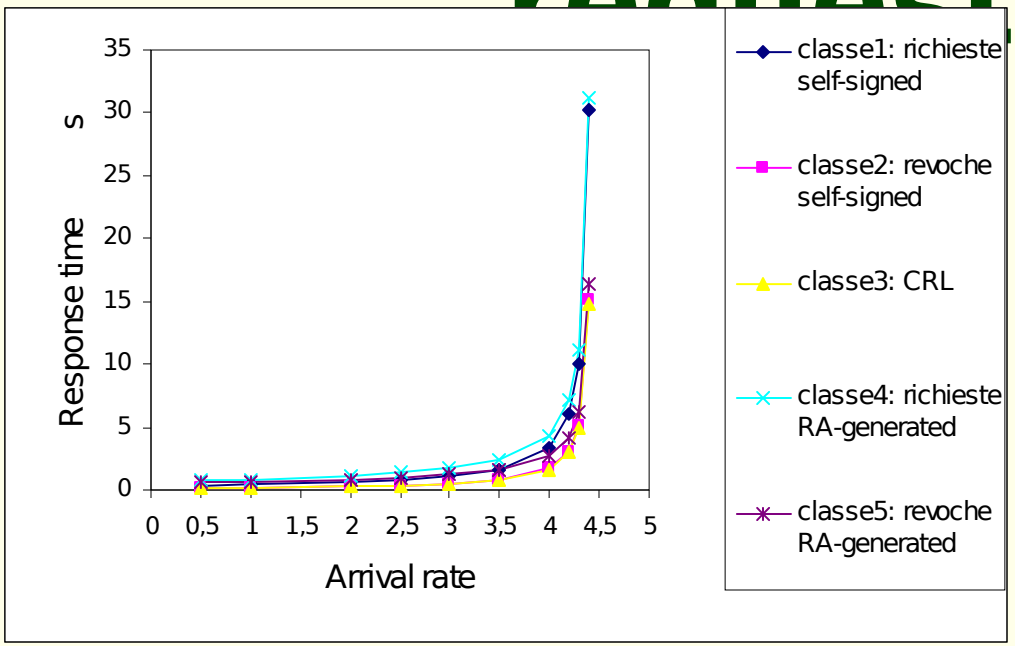
self-signed only requests

$2.5 < \lambda_{max} < 3.5$

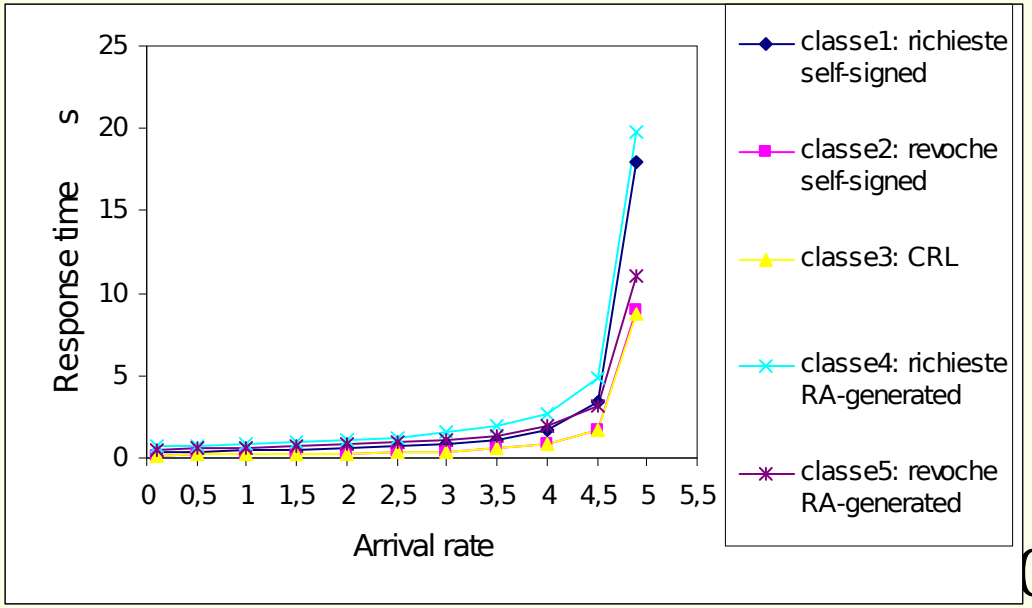
Model results

- Revocation requests rate larger than certificate requests rate
  - very unbalanced: tot. revocation fraction 82%
    - $\forall \beta_1 = \beta_4 = 9\%$
    - $\forall \beta_2 = \beta_5 = 41\%$
  - less unbalanced: tot. revocation fraction 66%
    - $\forall \beta_1 = \beta_4 = 17\%$
    - $\forall \beta_2 = \beta_5 = 33\%$

More revocation requests



66% revocation requests
$4 < \lambda_{max} < 4.5$



82% revocation requests
$4.5 < \lambda_{max} < 5$

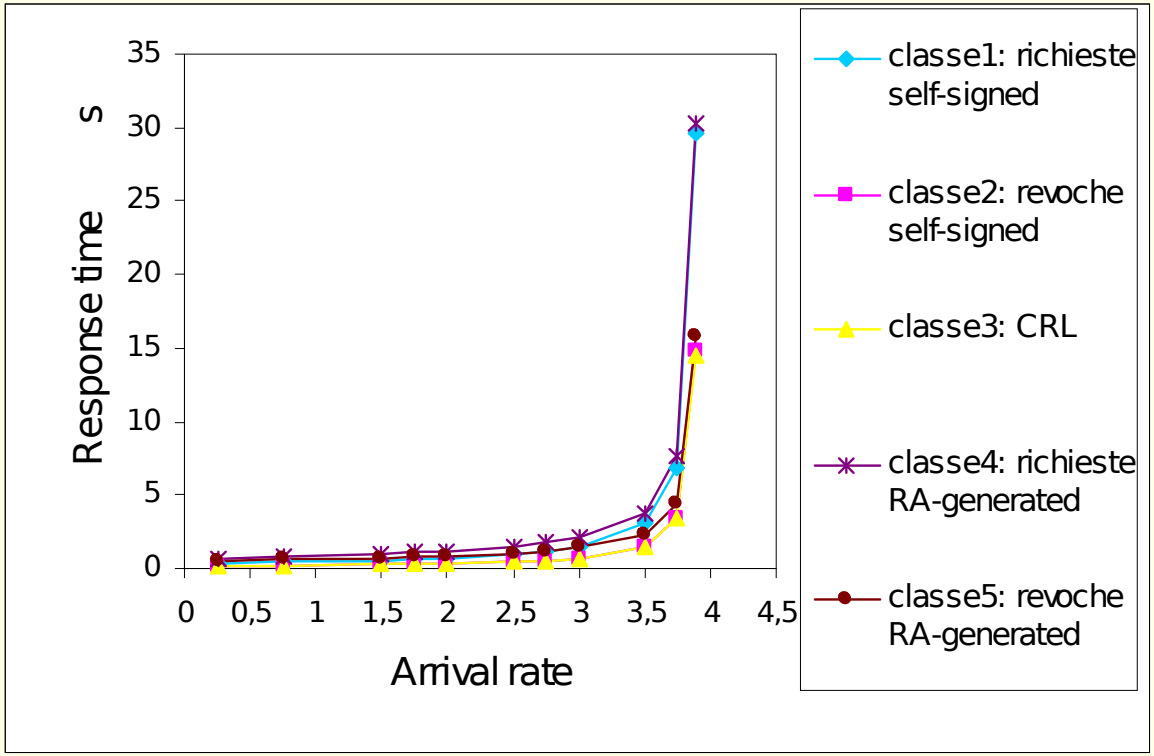
Resti/DSI

Model results

- Balanced load
  - $\beta_1 = \beta_2 = \beta_4 = \beta_5 = 25\%$
  - with λ - λ_3 such that response time is less than 5s, N ≈ 755,000
    - $C_{rev} = 151{,}000$
    - S_{CRL} = 1.3MB, average size of a full CRL
      - $S_{CRL} = 51 + 9*C_{rev}$ B
    - T_{CRL} = 0.568 s, time to generate a full CRL
      - $T_{CRL} = T_{disk} + T_{hash} + T_{sig}$

      irrelevant since performed every 4 hours

Balanced load

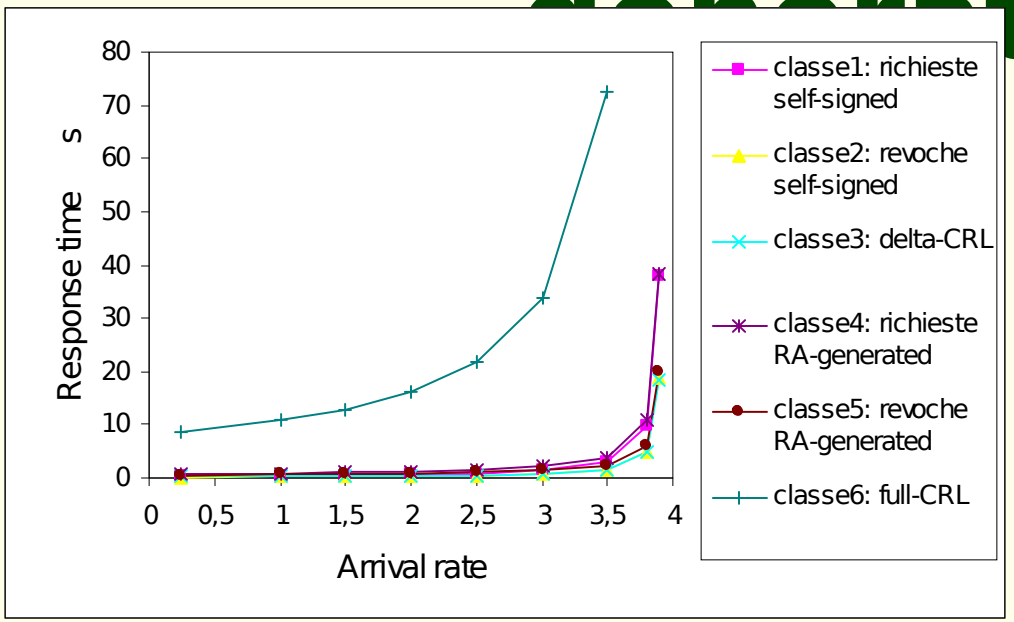


$3.5 < \lambda_{max} < 4$

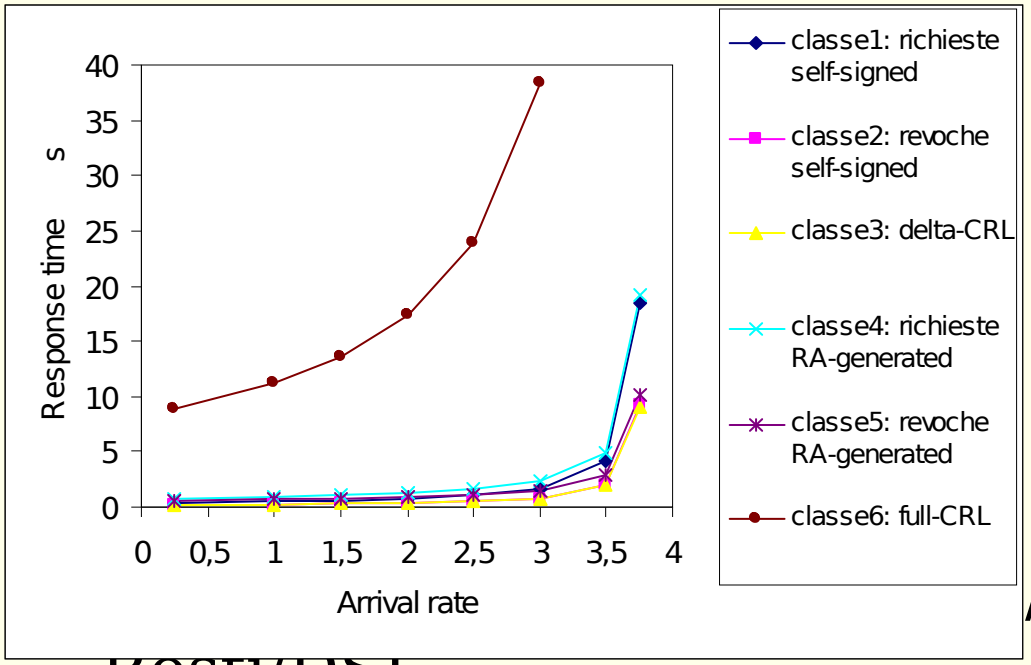
Model results

- Balanced load
  - $\beta_1 = \beta_2 = \beta_4 = \beta_5 = 25\%$
  - λ max = 3.5 req/s, Resp-Time < 5s
- Limit frequency of full CRL publication without affecting performance
  - 5 minutes
- Limit frequency of delta-CRL publication without affecting performance
  - 1 minute

Impact of full CRL generation



$\lambda_6 = 0.00007$ once every 4 hours



variable λ_6

Model results

- Signed log files
  - each operation performed by CA logged
  - CA signs each file entry
  - service times per class (s)

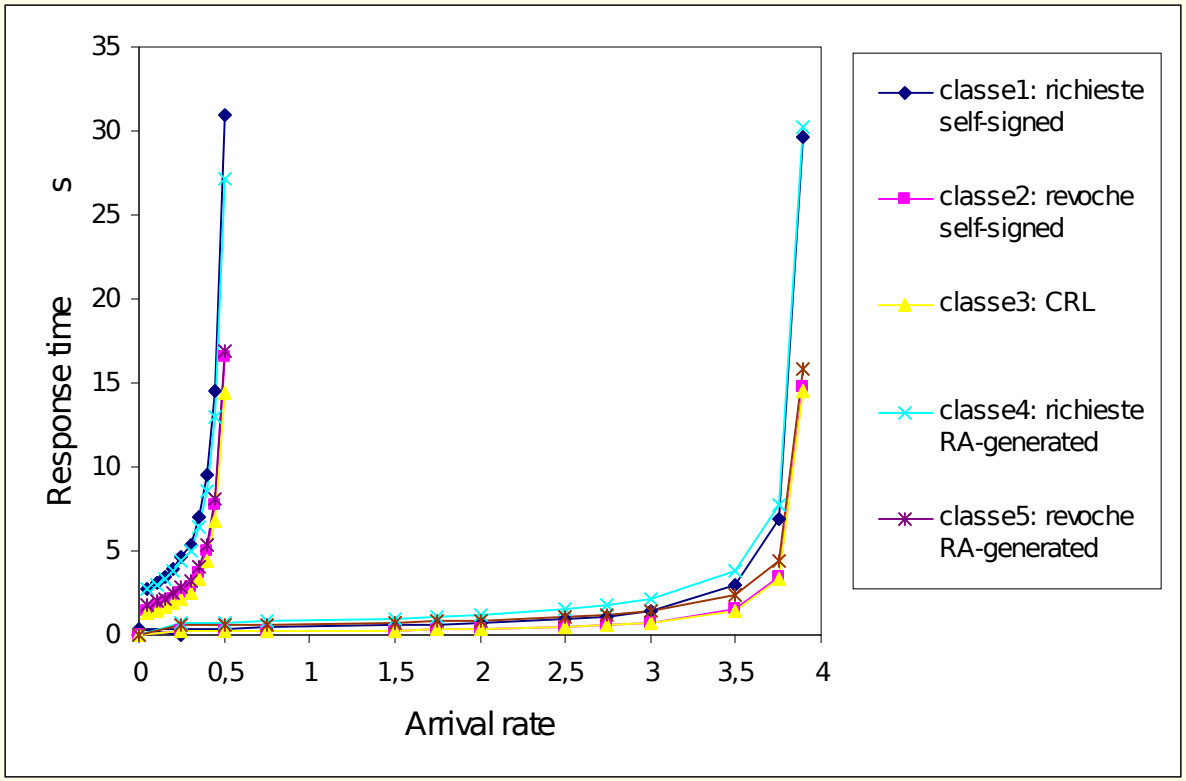
	cl1	cl2	cl3	cl4	cl5
CA	2.498	1.332	1.162	2.162	1.332

cl1: self-sig. req.
cl2: self-sig. rev.
cl3: delta-CRL
cl4: RA-gen req.
cl5: RA-gen rev.

Signed log file

- Unbalanced load
  - $\beta_1 = \beta_4 = 41\%$, $\beta_2 = \beta_5 = 9\%$
    - $\forall \lambda_{max} \approx 0.4$ req/s
  - $\beta_1 = \beta_4 = 17\%$, $\beta_2 = \beta_5 = 33\%$
    - $\forall \lambda_{max} \approx 0.66$ req/s
- Balanced load
  - $\beta_1 = \beta_4 = \beta_2 = \beta_5 = 25\%$
    - $\forall \lambda_{max} \approx 0.5$ req/s

Plain vs signed log files



$\lambda_{sat} \approx 0.5$ vs 3.7 req/s

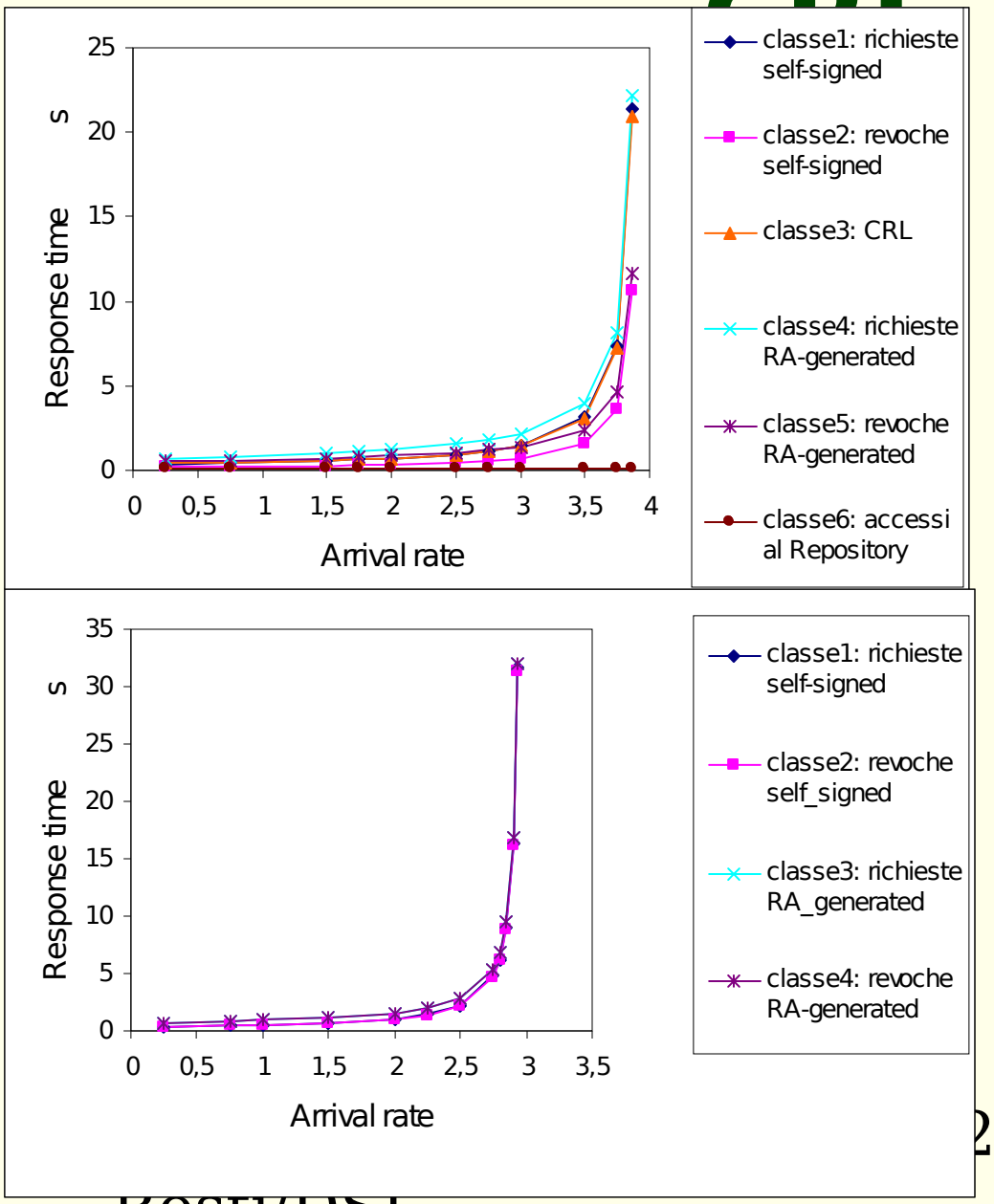
Enhancements

- Directory requests according to [Cooper2000]
  - sliding window over-issued delta-CRL
    - full CRL every 20 hours
    - delta-CRL every ten minutes, valid for 4 hours
  - directory utilization increases
  - λ_{max} not affected

Enhancements

- Revocations are signed and immediately published
  - users query the repository directly – no CRL
  - $2.5 < \lambda_{max} < 3$ req/s with balanced and unbalanced load

Over-issued CRL vs no CRL



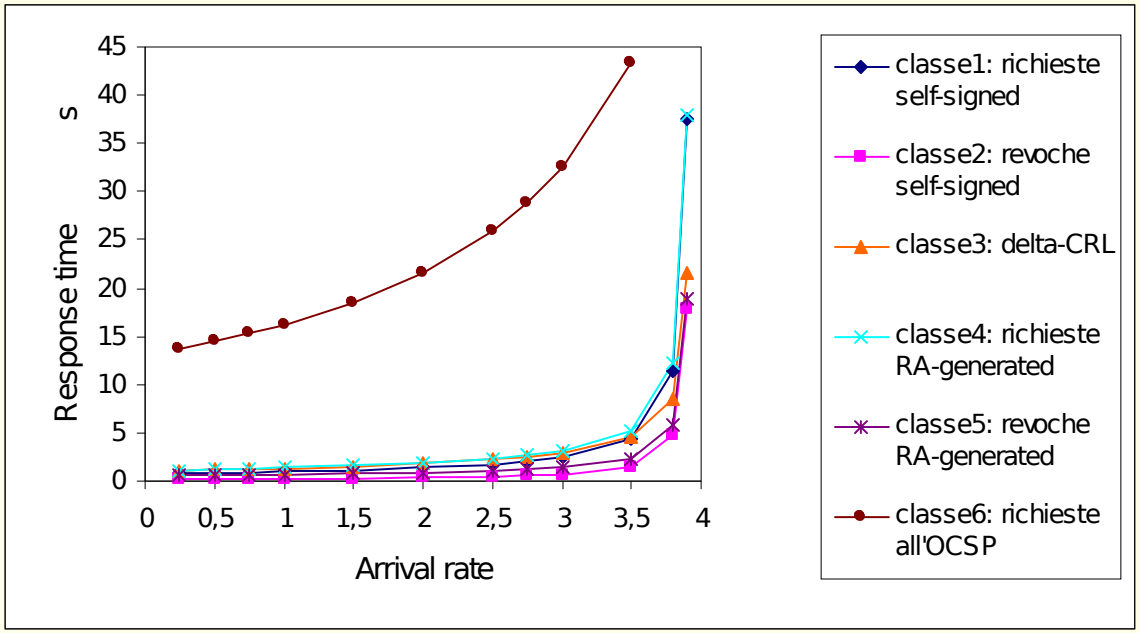
Over-issued CRL w/ balanced load

revocations signed individually balanced load

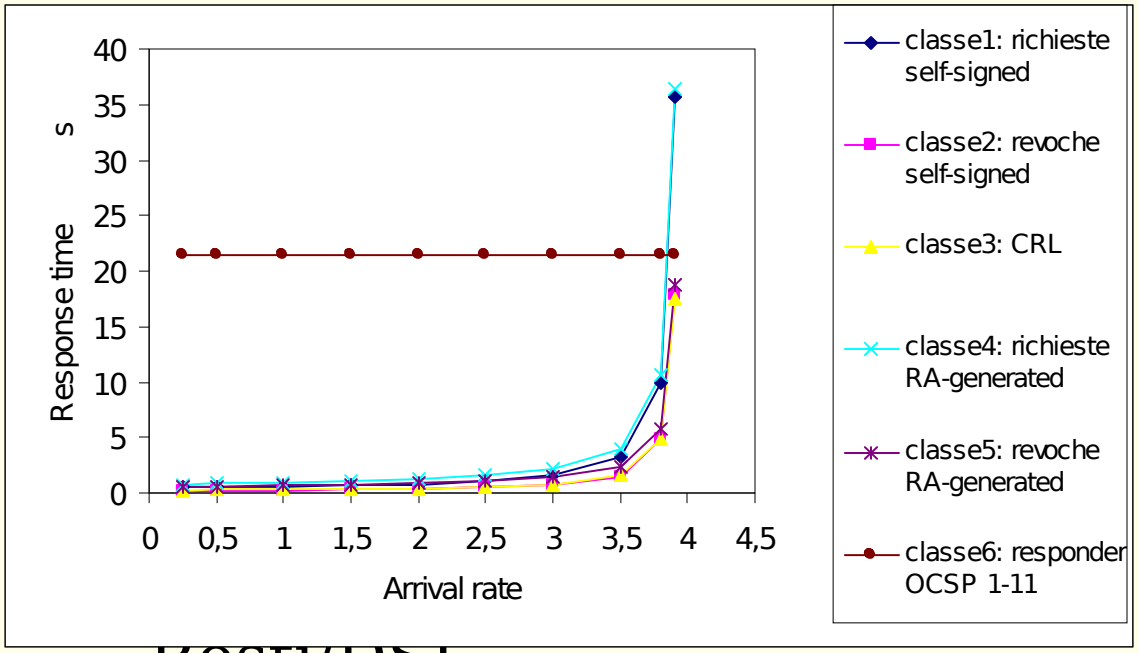
Enhancements

- Online Certificate Status Protocol
  - users query OCSP responder
  - only OCSP responder downloads CRL
  - OCSP signs replies to users
  - $\lambda_{max\_OCSP} \approx 5.67$ query/s
  - $3.5 < \lambda_{max} < 4$ req/s with balanced load

OCSP



single OCSP



11 OCSP server

1

Future work

- Compare results with software-only systems
  - no cryptographic coprocessor used
- Include communication time
  - bottleneck might switch
- Add Timestamp Authority
- Estimate total number of users for a given performance level

Bibliography

- Cooper1999: D.A. Cooper, A model of certificate revocation, 15th Annual Computer Security Application Conference, pp 256-264, 1999.
- Cooper2000: D.A. Cooper, A more efficient use of delta-CRL, 2000 IEEE Symposium of Security and Privacy, pp 190-202, 2000.